

### **REMARKS**

Applicant respectfully requests reconsideration. Claims 1-42 were previously pending in this application. Following the amendment, claims 1-42 are pending for examination with claims 1, 14, 21, 34, 41, and 42 being independent claims. No new matter has been added.

#### **Rejections Under 35 U.S.C. §102**

Claims 1-42 are rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Nyman et al., U.S. Published Patent Application No. 2003/0037033.

In light of the amendments to the claims, Applicants respectfully request that the rejection be withdrawn.

As an aid to the Examiner, Applicants present a brief summary of the Specification and the Nyman reference. This summary is not intended as a substitute for the Examiner reading the application or the reference in its entirety. Further, this summary is not intended to characterize the claims or any limitations of the claims, which are discussed individually below.

Briefly, the present application relates to a peer-to-peer collaboration system [01]. In such a peer-to-peer collaboration system, collaborating devices, such as the two devices shown in Fig. 1A, exchange data change requests, called “deltas” [35]. The exchange of deltas is illustrated by arrow 106 in Fig. 1A. Because deltas may be transmitted over an unsecure medium, such as the Internet, the peer-to-peer collaboration system uses authentication and encryption techniques to insure confidentiality and data integrity [41]. As new collaboration members join the peer-to-peer collaboration session, encryption keys may be exchanged between collaborating members that can be used to transmit information securely [53].

However, one way that security may be defeated is if a user is “spoofed” into thinking that he or she is communicating with an authorized user, when in fact he or she is communicating with an unauthorized user [54]. This scenario may occur, for example, if the unauthorized user attempts to join the peer-to-peer collaboration session using a display name that is equivalent to the display name of the authorized user. One of the collaborating users may mistakenly communicate with the unauthorized user.

To avoid such a breach of security, the present application describes that when the peer-to-peer collaboration system offers a user an opportunity to select a contact with which to

communicate, the system displays relevant status information about contacts to be selected. For example, the display provided by the system may include information about whether the contact has been authenticated or certified. Or, the status information may notify a user that there are potentially multiple contacts having equivalent display names.

Fig. 4 provides an example of icons that may be displayed in conjunction with the display names of other contacts to communicate this status information. For example, 400 is an icon that may be used to indicate a contact has been manually authenticated. Icon 402 may be used to indicate a contact that was certified based on that contact's association with the same enterprise as the user. Icon 404 may indicate a user in a managed domain, though a managed domain outside the user's organization. Icon 406 may be used to indicate a contact that has a name equivalent to another contact the user maintains.

The present application describes multiple ways that this status information may be used. For example, Fig. 5B indicates information that may be presented to a user when attempting to initiate a communication function with a contact for which another contact exists having an equivalent name. Fig. 5C illustrates the result of a conflict resolution process that can be performed by the system described in the present application. As can be seen by comparison of the two figures, the user has been allowed to change the names used to display contacts that had equivalent names. Accordingly, Fig. 5C shows that both contacts appear with different display names and no longer are displayed with icons such as 504 and 506 indicating a display name conflict. An example of processing used by the system to move from a display as shown in Fig. 5B to the display as shown in Fig. 5C is described in conjunction with the flow chart of Fig. 6 and pictured graphically in Figs. 7, 8 and 9.

Another aspect of maintaining security in a peer-to-peer collaboration system relates to limiting communication with contacts that are either unauthenticated or uncertified. The specific actions that may be allowed or disallowed may be specified in a security policy. The present application describes that a security policy may restrict communication or warn a user of an attempt to communicate with a contact that would violate the security policy, which creates an option for the user to choose whether to continue with the communication. Figs. 10 and 11 provide examples of graphical user interfaces through which security policies may be established. Fig. 12 is flowchart of a process through which the security policies may be applied in practice.

In contrast, the Nyman reference describes a method of allowing devices connected in an ad hoc network to identify themselves to other devices within the ad hoc network. The reference describes a “name distribution message” (see Abstract). The reference describes that the name distribution message may be passed from device to device in the ad hoc network so that all interconnected devices may learn the names for all other devices.

The Nyman reference describes a conflict resolution system that occurs automatically to prevent errors of multiple devices providing the same name. To avoid conflicts, the user of each device may specify multiple names and every other device may execute an algorithm to select one of those names to ensure that every device selects the same unique name for each other device.

The Nyman reference also describes that security attributes may be transmitted as part of the name distribution message. However, the security attributes are implemented by encrypting the names in the name distribution message using public keys from only those devices intended to be able to display the device name. Consequently, devices that are not intended to display the name of another device are not able to decrypt its name and so cannot display it.

Thus, there are at least two distinctions between the system of the Nyman reference and the system described in the present application. First, all of the information relating to device aliases and security is specified for a device by the user of that device. This approach is opposite of what is described in the present application in which users who want to communicate with a device establish an alias for that device and apply their own security policy. Accordingly, the reference is unrelated to creating a security policy to block users from communicating, intentionally or unintentionally, with unauthorized users because the unauthorized user could simply set security attributes for its device to allow communications with all users.

A second important difference is that the process described in Nyman is automatic and occurs without user interaction. For example, paragraph 25 of the reference describes an algorithm that is used to select an alias that involves no user action.

Turning specifically to the claims, Claim 1 recites a method that involves displaying a name conflict indicator on a graphic user interface. The claim further recites actions that occur “in response to user input associated with the name conflict indicator.” Element (c) of the claim further recites receiving user input. Because Nyman describes an automatic system, the steps relating to user input and output do not occur. Further, because the user of each device sets

aliases for its device in advance of there ever being a conflict, there is no teaching or suggestion of “displaying a name conflict indicator.”

Independent claim 21 is an apparatus claims. But, the claim similarly recites limitations relating to display of a name conflict indicator. The claim further recites apparatus for input and output on a graphic user interface. For reasons described in connection with claim 1, Nyman does not teach or suggest these limitations.

Independent claim 41 recites a computer program product containing program code for displaying on a graphical user interface information in conjunction with a name conflict indicator and also receiving user input associated with the name conflict indicator. For reasons described in connection with claim 1, Nyman does not teach or suggest these limitations.

As to claim 14, the claim also recites multiple limitations that are not met by the system of Nyman. For example, claim 14 recites “receiving through a graphic user interface an indication of a selected contact.” The claim further recites “obtaining the authentication and certification level of the selected contact.” These limitations cannot be met in combination by the system of Nyman. The security attributes described in the reference block the display of information about a contact. Thus, there would be no authentication and certification level information available for a contact that could be displayed on, and therefore selected through, a graphic user interface. Consequently, there is no reasonable interpretation of the reference that simultaneously meets limitations (b) and (c) of the claim.

Further, the reference does not teach or suggest step (d) of claim 14. The security attribute in the reference is used to block display of information about a contact from being displayed. The system of the reference does not warn the user and restrict the user from communicating with a selected contact that was displayed. Consequently, there is no reasonable interpretation of the reference that simultaneously meets limitations (b) and (d) of the claim.

Claims 34 and 42 recite limitations that, for reasons described in connection with claim 14, are not shown or suggested by the reference.

The remaining claims depend directly or indirectly from one of the independent claims. For at least the reasons given above, the dependent claims distinguish the reference. Accordingly, the rejection should be withdrawn.

**CONCLUSION**

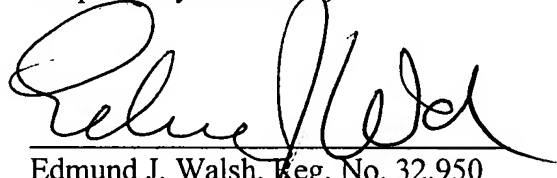
A Notice of Allowance is respectfully requested. The Examiner is requested to call the undersigned at the telephone number listed below if this communication does not place the case in condition for allowance.

If this response is not considered timely filed and if a request for an extension of time is otherwise absent, Applicant hereby requests any necessary extension of time. If there is a fee occasioned by this response, including an extension fee, that is not covered by an enclosed check, please charge any deficiency to Deposit Account No. 23/2825.

Dated: March 23, 2007

Respectfully submitted,

By:

A handwritten signature in black ink, appearing to read 'Edmund J. Walsh', written over a horizontal line.

Edmund J. Walsh, Reg. No. 32,950  
Wolf, Greenfield & Sacks, P.C.  
600 Atlantic Avenue  
Boston, Massachusetts 02210-2206  
Telephone: (617) 646-8000